أمن الحاسوب الشخصي

أعداد المبرمج:مشتاق طالب رشيد العامري

16-12-2009

بعض طرق الوقاية من الأختراق الألكتروني



طريقة اكتشاف البورتات المفتوحة في جهازك

البورت هي البوابة التي تمكن الهاكر من الدخول إلى جهازك، لذلك يجب عليك أن تعرف هذه البوابة وتقوم بإغلاقها. وسنذكر الطريقة التي تكشف لك البوابات (البورتات) المفتوحة في جهازك.

تتم هذه الطريقة باستعمال الدوس.. قم بتشغيل الدوس بعدها أدخل الأمر التالي:

a-Netstat

ثم اضغط enter

عند تنفيذ الخطوات السابقة سيتم عرض جميع المنافذ المفتوحة وهي التي تلي الرمز (:) أما ما قبل الرمز فهو اسم الكمبيوتر الخاص بك الذي تم تعريفه عند تجهيز شبكة الاتصال.

```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    khalel:17300           0.0.0.0:0              LISTENING
  TCP    khalel:1039            0.0.0.0:0              LISTENING
  UDP    khalel:1039            *:*

C:\WINDOWS>     البورتات المفتوحه
```

ملاحظة

:

إذا أردت أن تحصل على نتائج حقيقية يجب أن تكون متصلاً بالإنترنت.

قائمة بأرقام المنافذ (البورتات) التي تستخدمها برامج الإختراق المتعددة.

رقم المنفذ (Port)	اسم البرنامج
٢	Death
٢١	Net Administrator, Senna Spy FTP Server,
٢٣	Truva Atl
٢٥	NewApt
٤٨	DRAT
٥٠	DRAT

Hooker	٨٠
Net Controller	١٢٣
Infector	١٤٦
Infector	(UDP) ١٤٦
Secret Service	٦٠٥
Aim Spy	٧٧٧
Der Spacher 3	١٠٠٠
Der Spacher 3	١٠٠١
Vampire	١٠٢٠
MiniCommand	١٠٥٠
WinHole	١٠٨٠
RAT	١٠٩٥
RAT	١٠٩٧
RAT	١٠٩٨
RAT	١٠٩٩
NoBackO	(UDP) ١٢٠٠
NoBackO	(UDP) ١٢٠١
SoftWAR	١٢٠٧
NETrojan	١٣١٣
OpC BO	١٩٦٩
Der Spaeher 3	٢٠٠٠
Der Spaeher 3	٢٠٠١
Xplorer	٢٣٠٠
The Prayer	٢٧١٦
SubSeven	٢٧٧٣
Terror Trojan	٣٤٥٦
Virtual Hacking Machine	٤٢٤٢
NetMetropolitan	٥٠٣١
PC Crasher	٥٦٣٧
PC Crasher	٥٦٣٨
Secret Service	٦٢٧٢
ScheduleAgent	٦٦٦٧
Host Control	٦٦٦٩
SubSeven	٦٧١١
SubSeven	٦٧١٢
SubSeven	٦٧١٣

2000 Cracks	٦٧٧٦
SubSeven	٧٠٠٠
SubSeven	٧٢١٥
Back Orifice 2000	٨٧٨٧
HackOffice	٨٨٩٧
Rcon	٨٩٨٩
The Prayer	٩٩٩٩
Syphillis	١٠٠٨٦
Ambush	**(UDP)** ١٠٦٦٦
Host Control	١١٠٥٠
Secret Agent	١١٢٢٣
BioNet	١٢٣٤٩
DUN Control	**(UDP)** ١٢٦٢٣
Mosucker	١٦٤٨٤
ICQ Revenge	١٦٧٧٢
Nephron	١٧٧٧٧
ICQ Revenge	١٩٨٦٤
Chupacabra	٢٠٢٠٣
Bla	٢٠٣٣١
SubSeven	٢٧٣٧٤
SubSeven	٢٧٥٧٣
Acid Battery	٣٢٤١٨
Trinoo	**(UDP)** ٣٤٥٥٥
Trinoo	**(UDP)** ٣٥٥٥٥
YAT	٣٧٦٥١
Acid Battery 2000	٥٢٣١٧
SubSeven	٥٤٢٨٣
NetRaider	٥٧٣٤١
Bunker_Hill	٦١٣٤٨
Bunker_Hill	٦١٦٠٣
Bunker_Hill	٦٣٤٨٥
The Traitor	٦٥٤٣٢
The Traitor	**(UDP)** ٦٥٤٣٢

طريقة إغلاق البورتات المفتوحة

سبق وأن تطرقنا إلى طريقة الكشف عن البورتات (المنافذ) المفتوحة في جهازك، والآن سنتعرف على طريقة إغلاق هذه المنافذ.

إنها مشكلة معروفة ومعتادة.. تنفذ أمر " netstat-a" على الويندوز، وترى عدد من المنافذ بحالة "LISTENING" أو "ESTABLISHED".

يعني ذلك أن بعض التطبيقات تعمل متخفية وبالتالي تُبقي المنافذ التي تستخدمها مفتوحة لأي اتصال قادم.

تكمن المشكلة في معرفة أيّ تطبيق هو الذي يبقي المنفذ مفتوحاً، ومن ثم يتم إغلاق هذا التطبيق.

فمن غير معرفة ذلك، يمكن أن يكون تروجان بداخل جهازك ويتم السيطرة عليه، أو غيره من التطبيقات التي تعمل دون علمك.

و لذلك يجب عليك التحرّي لمعرفة ما يُنصت في جهازك.

<u>استخدام Inzider :</u>

<!--[if !supportEmptyParas]--> Inzider هو برنامج بسيط يمكّنك من عرض جميع التطبيقات الفعّالة بالجهاز وأرقام المنافذ (البورتات) التي تستخدمها.

يمكنك تحميله من المواقع التالية: اضغط هنا للتحميل ((١)) ((٢))

[Inzider v1.2: 250 KB]

* <u>ملاحظة</u>: قد تظهر لك الرسالة التالية بعد التحميل:

"GkWare SFX Module V1.90/ Is -The data section attached to this self-extractor has been damaged. Please download this file again to get a complete copy."

عند ظهورها يجب عليك إعادة تشغيل الجهاز وتشغيل ملف التحميل مرة أخرى.

<u>**مثال** حول طريقة العمل:</u>

a -WINDOWS> netstat :C

> Active Connections [-supportEmptyParas!if]--!<

> Proto Local Address Foreign [-supportEmptyParas!if]--!< Address State

137 :>TCP gwen[-supportEmptyParas!if]--!< 0 LISTENING:GWEN

0 LISTENING :138 GWEN:TCP gwen

TCP gwen:nbsession GWEN:0 LISTENING

0 LISTENING :tftp GWEN:UDP gwen

*:*nbname :UDP gwen

*:*nbdatagram :UDP gwen

<[-supportEmptyParas!if]--!> في الأعلى يظهر لنا أن IP/NetBIOS قد تم تفعيله (المنافذ ١٣٧، ١٣٨، nbsession، nbname، nbdatagram).

مما يعني أن الجهاز يستخدم كسيرفر سامحاً للأجهزة بالشبكة في مشاركة الملفات أو استخدام الطابعة مثلاً.

ولكن يظهر لنا أيضاً TFTP (البورت 69/UDP) مفتوح، وذلك غريب بعض الشيء! حيث أن TFTP اختصار لـ (Trivial File Transfer Protocol) تعني أنه يسمح لإرسال واستقبال الملفات من غير رقيب.

لمعرفة ما هو سبب بقاء ال TFTP مفتوحاً.. نستطيع تشغيل برنامج Inzider ونجعله يقوم بتحليل النظام. النتيجة ستظهر إلى حدّ ما هكذا:

-1999, Arne Vidstrom (c) -1 .inzider 1
/inzider/toolbox/~winnt/se.bahnhof.www//:http

Checked <[-supportEmptyParas! if]--!> .(4294965459=PID) EXE.WINDOWSEXPLORER:C

.(4294841743=PID) EXE.WINDOWSTASKMON:Checked C

SYSTEMSCISCO TFTP PROGRAM FILESCISCO:Checked C .(4294857879=PID)EXE .SERVERTFTPSERVER

PROGRAM FILESCISCO :0 by C.0.0.Found UDP port 69 bound at 0 EXE.SYSTEMSCISCO TFTP SERVERTFTPSERVER

[client UDP] (4294857879=PID)

.(4294953443=PID)EXE .WINDOWSSYSTEMMPREXE:C Checked

.(4294916979=PID)DLL .WINDOWSSYSTEMKERNEL32:C Checked

.(4294845915=PID)EXE .WINDOWSSYSTEMSYSTRAY:C Checked

EXE .MCAFEEVIRUSSCANVSHWIN32:C Checked .(4294944083=PID)

.(4294869135=PID)EXE .WINDOWSSTARTER:Checked C

يُلاحظ أن "Inzider" وجد العديد من التطبيقات الفعّالة. PID يرمز إلى (Process ID) المستخدم من قبل النظام لتعريف وتمييز التطبيق الفعّال عن غيره من التطبيقات التي تعمل في نفس الوقت.

في الأعلى نجد أن هناك تطبيق واحد تنفيذي وهو EXE.TFTPSERVER والموجود في C: PROGRAM FILESCISCO SYSTEMSCISCO TFTP SERVER . وقد أظهر البرنامج أن المنفذ الذي يستخدمه هو (69/UDP) وهو منفذ الـ (TFTP).

بذلك وجدنا الملف التنفيذي الذي يشغل البورت ٦٩ التابع لـ TFTP، وهو ما أردنا الوصول إليه.

الآن لنا الخيار في إزالة هذا الملف ومنعه من استخدام البورت المخصص له، أو البقاء عليه إن علمنا أننا نريد الخدمة التي يقدمها.

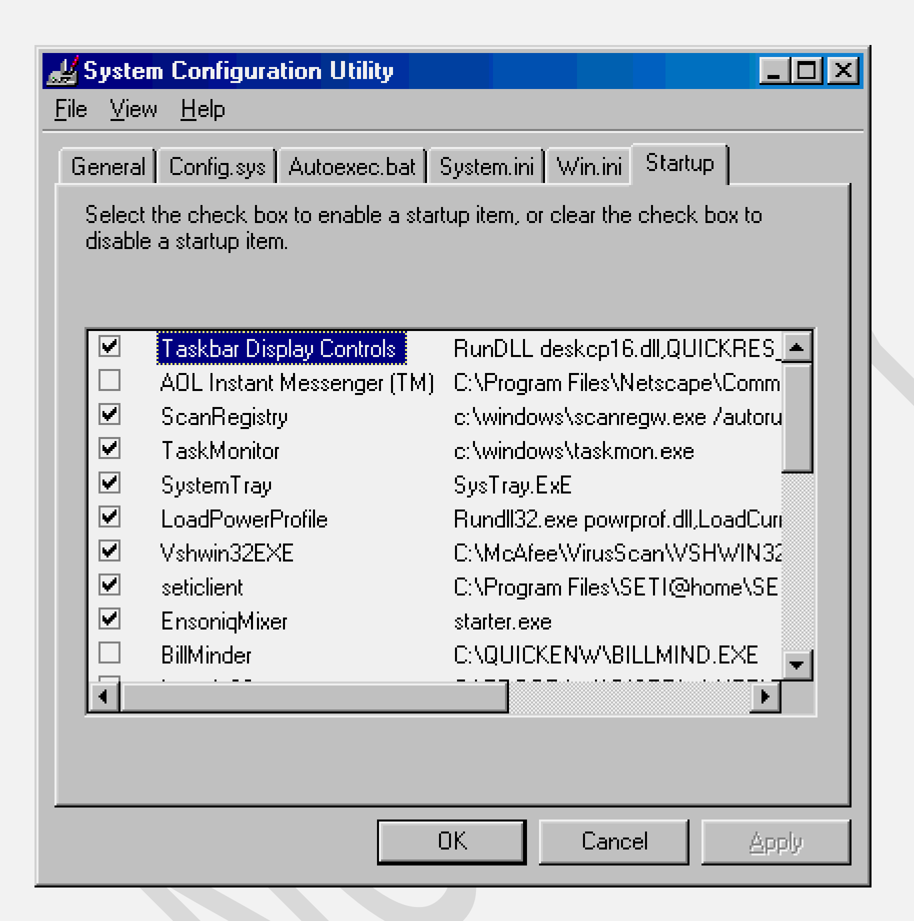
--!> <[-supportEmptyParas! if]--!> <[-supportEmptyParas!if]--!> <[-endif]

التحقق في Windows98:

ويندوز يضم أداة مميزة لمعرفة جميع التطبيقات التي تعمل عند تشغيل النظام. هذه الأداة هي الـ (System Configuration Utility) ويمكن الوصول إليها عن طريق C:exe.WindowsSystemMSConfig ، أو من خلال:

قائمة ابدأ Start > تشغيل Run > كتابة Msconfig . أو اضغط هنا للوصول إليها تلقائياً.

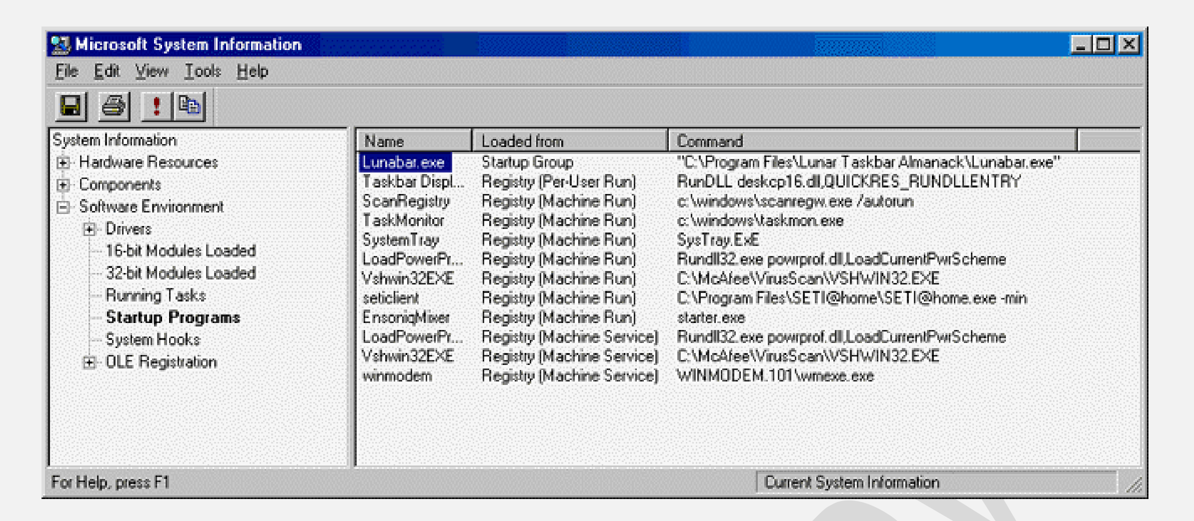
بعد التشغيل.. ننتقل إلى لسان التبويب (Startup) الذي يعرض جميع التطبيقات التي تعمل بمجرد تشغيل النظام. لمنع برنامج من التشغيل ببساطة قم بإزالة علامة التحديد بجانب اسمه، ثم OK. بعد إعادة التشغيل لن يتم تشغيل التطبيق الذي قمت بإزالته.



<[-supportEmptyParas!if]--!> إضافة إلى Startup Tab.. يمكنك عرض ملفات ال autoexec.config, system.sys, win.bat and ini.ini . واتباع نفس الطريقة في إيقاف التطبيقات الغير مرغوبة من التنفيذ. لسان التبويب General يمكنك من عمل نسخة احتياطية للملفات المشار إليها.

أداة أخرى مميزة في الويندوز هي (Microsoft System Information).

بعد تشغيلها من خلال نفس خطوات تشغيل وإنما كتابة عند تشغيل Msinfo32 أو اضغط هنا للوصول إليها مباشرة.. يتم الانتقال إلى Software Enviornment ثم Startup Programs .



<[-supportEmptyParas!if]--!> تقوم هذه الأداة بنفس عمل Msconfig من حيث معرفة التطبيقات التي تعمل عند بداية التشغيل، إنمّا يضاف على ذلك هنا أنه يمكن عرض من أين تمّ تحميل التطبيق (registry, .bat, etc.startup group, autoexec).

ويعدّ ذلك مفيداً في تحديد مكان التطبيق المراد إزالته دون البحث عنه.

<[-endif]--!> <[-supportEmptyParas! if]--!>

<u>الـخـلاصـة</u>:

- يتم كشف المنافذ المفتوحة عن طريق الأمر a-netstat في الدوس من خلال Start > Programs > Arabic DOS Windows أو غيرها من الطرق المعروفة للانتقال إلى الدوس.
- عند تنفيذ الأمر a- netstat لا بدّ وأن تظهر لك العديد من المنافذ إمّا بحالة Listening أو Established .. عندها يجب عليك التمييز بين التطبيقات التي تحتاجها مثلاً كالإكسبلورر والآوتلووك .. الخ. وملاحظة التطبيقات الغريبة خصوصاً إذا **ظهر لك رقم IP غير** معروف بالنسبة لك.. فهذا يعني أن هناك اتصال بين جهازك وآخر من خلال هذا التطبيق ويجب عليك غلقه وحذفه، إن لم تكن تستخدمه.

- مثال:

```
C:\WINDOWS>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    sfz:0                  0.0.0.0:0              LISTENING
  TCP    sfz:1032               0.0.0.0:0              LISTENING
  TCP    sfz:pop3               0.0.0.0:0              LISTENING
  TCP    sfz:2940               0.0.0.0:0              LISTENING
  TCP    sfz:2941               0.0.0.0:0              LISTENING
  TCP    sfz:1025               0.0.0.0:0              LISTENING
  TCP    sfz:1026               0.0.0.0:0              LISTENING
  TCP    sfz:1038               0.0.0.0:0              LISTENING
  TCP    sfz:2848               0.0.0.0:0              LISTENING
  TCP    sfz:2913               0.0.0.0:0              LISTENING
  TCP    sfz:1032               msgr-ns15.msgr.hotmail.com:1863  ESTABLISHED
  TCP    sfz:2940               proxy.isu.net.sa:8080  ESTABLISHED
  TCP    sfz:2941               proxy.isu.net.sa:8080  ESTABLISHED
  UDP    sfz:1025               *:*
  UDP    sfz:1026               *:*
  UDP    sfz:1038               *:*
  UDP    sfz:2848               *:*
  UDP    sfz:2913               *:*
```

- في المثال السابق.. الوضع الطبيعي إلى حدّ ما يبدو هكذا، حيث أنه لا يوجد أي رقم IP غريب ولا يمكن معرفة مصدره.. وكذلك هناك منفذ ال POP يمكن أن يكون مشغولاً إذا كنت تستخدم الآوتلوك لجلب ، وكذلك الماسينجر، ولا داعي للقلق خوفاً من التجسس في هذه الحالة. أيضاً تلاحظ وجود البروكسي لمزود الخدمة لديك.

- لإغلاق المنافذ (البورتات) الخطرة لديك.. يجب عليك أولاً: التعرّف على البرنامج الذي يستخدم هذا البورت من خلال برنامج Inzider. ثانياً: تتبع مصدر الخطر (ملف السيرفر) وحذفه.

- ينصح باستخدام أحد برامج الـ Firewall لحماية الجهاز. التي تعمل على إغلاق جميع المنافذ إلاّ المنافذ التي ترغب باستخدامها فقط كمنفذ POP للبريد أو منفذ الـ FTP .. الخ. وهذه البرامج عديدة ، أشهرها: Norton Internet Securtiy و Zone Alarm .

كعكة الإنترنت هل لديك الكثير منها؟

Internet Cookies

كعكة الإنترنت هي ملف نصي صغير مكون عادة من ستة أجزاء وهي: اسم الكعكة ، قيمتها ، تاريخ انتهاء مفعولها ، اتجاهها ، الموقع المالك لها، درجة الأمان (التشفير) وأخيرا طبيعة المعلومات التي تقوم بجمعها.
ومصدر هذه الكعكات هي المواقع التي تقوم بزيارتها أنت أثناء تجولك بالشبكة أو المواقع المتعاونه معها وهناك مصدر أخر وهو البريد الإلكتروني الخاص بك حيث أنك وحال فتحك لأي رسالة قادمة من أي مصدر يقوم ذلك المصدر باهدائك كعكة من انتاجه ! حتى لوكان المرسل صديق لك لأن كل صفحة مرسلة لابد من احتوائها على رموز مزود الخدمة لذلك الصديق خاصة إذا كانت الرسالة من النوع المكتوب بلغة الترميز

كيف ومتى تعمل؟

بكل بساطة ما أن تزور أي موقع على شبكة الإنترنت وتدخل على أي من صفحاتها الرئيسية كانت أو الفرعية حتى يقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة بهم واحدة تبقى في السيرفر الخاص بهم والأخرى يتم ارسالها لك وعادة يكرمونك بعدة كعكات حتى لاتقول عنهم بخلاء! ويقومون بارسال هذه الكعكات جاهزة ومطبوخة ولكن تنتظر منك بعض النكهات الخاصة بك حتى تكون كعكة معتبرة ومناسبة لذوقك! وذلك حال قيامك بتعبئة استمارة أو استبيان
ويقوم الموقع بتخزين الكعكة على قرصك الصلب في أحد الملفات مع العشرات أو المئات من الكعكات الاخرى التي قامت الموقع الأخرى بتخزينها من قبل دون أن تشعر أنت بذلك أو حتى الاستئذان منك! وفورا يتم اصدار رقم خاص ليميزك عن غيرك من الزوار وطبعا تبدأ الكعكة بأداء مهمتها التي أرسلت من أجلها ألا وهي جمع المعلومات وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات وهي عادة شركات دعاية وإعلان وكلما قمت بزيارة الموقع يتم ارسال المعلومات وتجديد النسخة الموجودة لديهم ويقوم المتصفح لديك بعمل المهمة المطلوبة منه مالم تقم أنت بتعديل وضعها كما سنرى في المقالة القادمة

المعلومات التي تقوم بجمعها المواقع

تختلف المعلومات من كعكة ألى أخرى حسب البرمجة الأساسية لها ولكن يمكن إيجازها في النقاط التالية: - نوع الجهاز والمعالج المستخدم - معرف بروتوكول الإنترنت الخاص بك - طريقة اتصالك بالإنترنت وسرعة المودم - المواقع التي تقوم بزيارتها - صفحاتك المفضلة- ماذا تشتري من

الشبكة- عما تبحث للشراء- ماهي الخدمات التي تبحث عنها- اهتماماتك على الشبكة وكم ساعة تقضي من الوقت على الشبكة- وكذلك اسمك وعنوانك البريدي وكافة المعلومات التي تقدمها للموقع وذلك أثناء تعبئة الاستمارات أو الاستبيانات- رقم بطاقة الإئتمان الخاصة بك وغيرها من المعلومات المفيدة

حقائق عن كعكة الإنترنت

هي ليست برامج بحد ذاتها ولكنها مجموعة من المعلومات المخزنه والمرتبة ولذلك هي لاتشكل تهديد أمني مباشر لجهازك وذلك لعدم مقدرتها على حمل أو نقل الفيروسات كما انها لا تستطيع جمع معلومات شخصية عنك غير التي تقوم أنت بنفسك بتقديمها للمواقع أثناء تعبئة الإستمارات أو نماذج التسجيل
الحقيقة الأخرى وهي أن هذه المعلومات لا يستطيع قراءتها والاستفادة منها سوى مصدرها لأنها عادة مشفرة إلا إذا كانت متعاقدة أو متعاونة من مواقع أخري لتبادل المعلومات فيما بينها
والحقيقة الأخري أن ليست كل الكعكات مخصصة لجمع المعلومات فهنالك كعكات تساعدك على اتمام عملية الشراء وأخرى تساعد على سرعة تحميل وتنزيل الصفحة عند تكرار الزيارة في المستقبل وذلك بتخزين الصور وغيرها من الملفات الكبيرة والتي عادة ما تأخذ وقت طويل لنقلها على الشبكة وهناك ما يساعد على تجنب تكرار الإعلانات وهناك ماهو مخصص للتعرف عليك وأداء التحية

كيف يمكنك ايقاف أو على الأقل ان تقلل من كمية الكعكات التي لا تتوقف عن ارسال المعلومات عنك؟

يمكنك ذلك بعدة طرق و أولها مسح تلك الكعكات المخزنة في قرصك الصلب بطريقة دورية ومسح تاريخ المواقع التي زرتها وكذلك يمكنك إزالة الملفات المؤقتة المتعلقة بالمتصفح الخاص بك. وهناك طرق اخرى للحيلولة دون تكرار زرع تلك الكعكات في قرصك الصلب وهي تعديل عمل المتصفح لديك أو شراء أحد البرامج المتخصصة في الحماية

دليل عملي على كيفية إزالة الكعكات من قرصك الصلب وكيفية منعها من التخزين مجددا

ننصح بطباعة الصفحة قبل الإستمرار

اولا : كيفية إزالة الكعكات من قرصك الصلب

قم بإغلاق متصفحك وإقطع الاتصال بالإنترنت وبعد ذلك انقر على مفتاح البداية وعندها تظهر لك قائمة البداية ، قم باختيار

Find "find Files or Folders "
type "cookies "
Look in "My computer "
press Find

تظهر لك جميع المجلدات تحت ذلك الاسم، قم يفتح كل مجلد وبعد ذلك

From Edit Menu "select all "
then from Edit Menu press "Delete "

كرر العملية نفسها مع جميع المجلدات بنفس الاسم، كما ننصح القيام بذلك كل فترة من الزمن
ملاحظة: قد يسألك الجهاز ... انها كعكات هل أنت واثق من رغبتك في إزالتها؟ أجب بنعم ولاعليك منها

ثانيا: لنقم بمسح الكعكات المخزنه لديك في الملف المؤقت الخاص بمتصفحك ، إذا كنت تستخدم انترنت إكسبلورر قم بالنقر على أيقونة المتصفح لديك مره واحدة بالزر الأيمن للفأرة وتظهر لك لائحة بها عدة خيارات، قم باختيار
Properties
then new window with different pages will open for you, select ""General ""
وهي تنقسم إلى ثلاث أجزاء وفي الجزء الأوسط تجد
Temporary Internet Files
إذا كنت ترغب بمسح الملفات مباشرة دون الاطلاع عليها قم بالضغط على

Delete file
يظهر لك سؤال عن رغبتك في مسح الصفحات المحفوظة للاطلاع عليها دون الاتصال على الشبكة ، قم باختيارها إذا لا تريد الاحتفاظ بها وفي النهاية اضغط
OK
أما إذا كنت ترغب في مشاهدة الكعكات ومصادرها قم بالضغط على
setting
View Files or View Object

وبعدها يمكنك العودة لمسحها كما تم شرحه أعلاه

وأخيرا قم بمسح ملف تاريخ زياراتك للمواقع وذلك بالضغط على
Clear History

كيفية تجنب تخزين الكعكات على قرصك الصلب

يمكنك التحكم بمتصفحك وذلك بعدم السماح له بتخزين الكعكات على قرصك الصلب واليك الطريقة

بنفس الطريقة قم بالضغط على أيقونة المتصفح وذلك بالزر الأيمن من الفأرة و اختر خصائص

Properties , select Security
then press on costom level
وقم بالنزول بالصفحة حتى تجد
cookies

وبها الخيارات التالية

-Allow cookies that are stored on your computer
وتحت هذا الخيار قم باختيار
Disable
حتى تمنع تخزين الكعكات على قرصك الصلب
-allow persession cookies)not stored (

قم باختيار
enable
وهذا الاختيار يعطيك ميزة السماح للكعكات والعمل مؤقتا عند تصفحك للإنترنت وبالتالى الاستفادة من جميع مميزات المواقع ولكن دون السماح بتخزين الكعكة حيث أنك وبمجرد اغلاق المتصفح سوف تتخلص من الكعكات ، أما إذا رغبت بعدم السماح لهم مطلقا قم باختيار
Disable
ولكن سوف لن تستطيع مشاهدة بعض الصور أو التمتع بجميع امكاتيات الصفحة
للانتهاء قم بالضغط على
OK
ولتهيئة المتصفح لديك للقيام بمسح الكعكات في كل مرة بعد انتهاءك من التصفح إذهب الى
Advanced

وعليك بالنزول بالصفحة حتى تجد

security
وقم باختيار
Empty Temporary internet files folder when browser is closed, then press OK

وطبعا لا تنسى أن تقوم بالتخلص وافراغ سلة المهملات من الكعكات التي قمت بمسحها من الملفات، لأنها وإن انتقلت إلى سلة المهملات على سطح المكتب إلا أنها تقوم بدورها مالم تتخلص نهائيا منها

طرق التخلص من ملفات التجسس

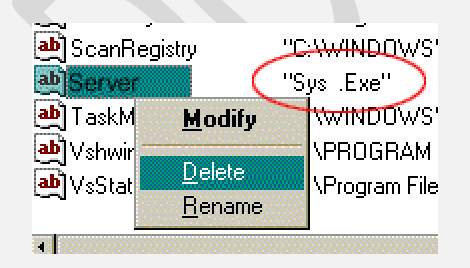


هذه مجموعة من اشهر ملفات التجسس و طرق الخلاص منها ..

Back Oriface

يعمل على فتح المنفذ ٣٣١٧ لجهازك و يجعل مستخدمي برنامج باك اورفز قادرين على اختراقك .

طريقة التخلص من الملف:



و Run اختر Start - من قائمة البداية1
اكتبRegedit
- من القائمة على اليسار اختر2
HKEY_LOCAL_MACHINE ثمSoftware ثم Microsoft ثم Windows ثم Current Virsion ثم Run أو احيانا Run Once.
لكن يمكنك Exe - اسم الملف متغيير من مكان لأخر امتداده دائما3 عندما exeمعرفته كون اسم الملف او السرفر تظهر بعده مسافةو من ثم . تجد الملف الغه تماما ..

- النسخ قبل ٢٠٠٠ Net Bus

هو الاكثر انتشارا على الشبكة .حجمه ٤٧٠ كيلو بايت
يستخدم المنافذ ١٢٣٤٥ و المنافذ ١٢٣٤٦و هو يمكن المخترق من السيطرة شبه الكاملة على جهازك .

طريقة التخلص من الملف:

1- اطفأ الجهاز و اعد تشغيلة بهيئة الوضع الآمن اوSafe Mode .
2- من الاعلى انتبع الخطوات من١و 2
3- ابحث عن الملف التالي c:\windows\patch.exe و الغه و من ثم اعد تشغيل الجهاز.

للأعلى

Net Bus 2000

على عكس السابق فاسمه متغيير و حجمة ٥٩٩ بايت.

طريقة التخلص من الملف:

1 من قائمة البداية Start- اختر Run واكتب Regedit
2- من القائمة على اليسار اختر HKEY_LOCAL_Machine ثم Software ثم Microsoft ثم Windows ثم Current Virsion ثم Run services
3- ابحث في القائمة على اليمين عن NBsvr.exe (هذا هو اسم الملف في الغالب) هكذا انت على علم ان جهازك مصاب .. و عليك بالعلاج التالي .وحتى و ان لم تجد الملف السابق اكمل الخطوات التالية.
4- انتقل إلى HKEY_LOCAL_USER ثم ابحث عن مجلد اسمه NetBus Server اختر بزر الفأرة الايمن اضغط على المجلد DELETE
5- اختر إعادة تشغيل الجهاز بوضع دوس DOS
5- اكتب Cd Winodw ثم إدخال اتبعها ب Enter CD system و ادخال و من Del NBSvr.exe و ادخال ثم اكتب Del NBHelp.dll، و اخي Del Log.txt و انتهى . اعد تشغيل جهازك .

Heack'a Tack'a

مما يصعب الوصول اليه.يستخدم المنافذ رقم FTP يستخدم بروتوكل ٣١٧٨٥ و ٣١٧٨٧ و ٣١٧٨٩ و ٣١٧٩١ .

طريقة التخلص من الملف:

1 من قائمة البداية Start- اختر Run واكتب Regedit
2- من القائمة على اليسار اختر HKEY_LOCAL_MACHINE ثم Software ثم Microsoft ثم Windows ثم Current Virsion ثم Run أو احيانا Run

و الذي يوافق المسار Explorer32 - ابحث عن3
و قم بحذفه C:\WINDOWS\Expl32.exe

للأعلى

NetSphere

يستخدم المنافذ TCP 30100 -TCP 30101-TCP 30102

طريقة التخلص من الملف:

Regeditو اكتب Run اختر Start- من قائمة البداية 1
Software ثم HKEY_LOCAL_MACHINE - من القائمة على اليسار اختر2
Run ثم Current Virsion ثم Windows ثم Microsoft ثم
c:\windows\system\nssx.exe -ابحث في الجهه اليمنى عن2
- احذف هذا الملف . و اعد تشغيل الجهاز بواسطه الضغط على3
CTRL+ALT+DELETE.

للأعلى

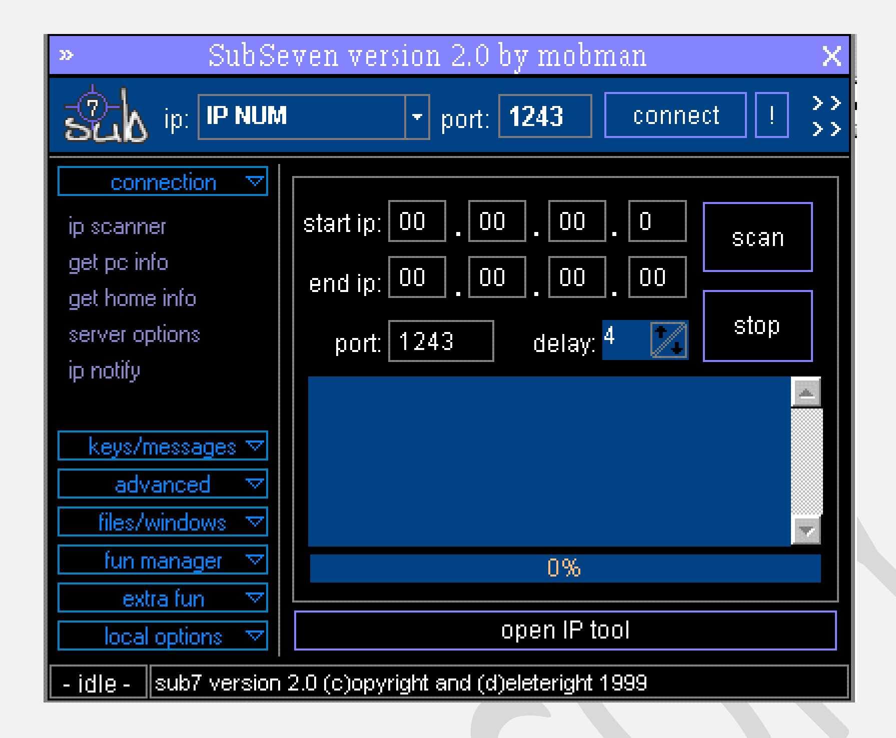
مصادر و برامج مفيدة:

- معلومات حول انواع كثيرة من ملفات Commondon Threat التجسس إذا لم تجد ما تريد في موقعنا يمكنك الاتجاه لهذا الموقع .
- يقوم بتنظيف جهازك من معظم ملفات التجسس. The Cleaner
- قائمة بالمنافذ المستخدمة من قبل ملفات التجسس Port list
- و انواع اخرى Back Oriface ينظف جهازك من BOClean

كيف تتخلص من القنبلة Sub seven

أخطر برامج الإختراق يسمى في منطقة الخليج (الباكدور جي) ويطلق عليه البعض إسم القنبلة تتركز خطورته في أنه يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه يعتبر أقوى برنامج إختراق للأجهزة الشخصية وفي إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة Mirc كما يمكنه إختراق أي جهاز أي شخص بمجرد معرفة إسمه في ICQ

أخطر برامج الإختراق يسمى في منطقة الخليج (الباكدور جي) ويطلق عليه البعض إسم القنبلة تتركز خطورته في أنه يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفهيعتبر أقوى برنامج إختراق للأجهزة الشخصية .. وفي إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة Mirc كما يمكنه إختراق أي جهاز أي شخص بمجرد معرفة إسمه في ICQ كما يمكنه إختراقمزودات البريد pop3/smtp يعتبر الإختراق به صعب نسبيا وذلك لعدم إنتشار ملف التجسس الخاص به في أجهزة المستخدمين الا أنه قائما حاليا على الإنتشار بصورة مذهلة ويتوقع أنه بحلول منتصف عام ٢٠٠١ سوف تكون نسبة الأجهزة المصابة بملف السيرفر الخاص به ٤٠-٥٥ % من مستخدمي الإنترنت حول العالم وهذه نسبة مخيفة جدا إذا تحققت فعلا ... مميزاته خطيرة للغاية فهو يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوي على أوامر كثيرة تمكنه من السيطرة عليه ... بل يستطيع أحيانا الحصول على أشياء لا يستطيع مستخدم الجهاز نفسه الحصول عليها مثل كلمات المرور .. فالمخترق من هذا البرنامج يستطيع الحصول على جميع كلمات المرور التي يستخدمها صاحب الجهاز !!! ولخطورته الكبيرة فسوف نفصل في الشرح عنه



أعـراض الإصابة :

من أهم أعراض الإصابة بهذا البرنامج ظهور رسالة " قام هذا البرنامج بأداء عملية غير شرعية ... " وتظهر هذه الرسالة عند ترك الكمبيوتر بدون تحريك الماوس أو النقر على لحة المفاتيح حيث يقوم البرنامج بعمل تغييرات في حافظة الشاشة وتظهر هذه الرسائل عادة عندما تقوم بإزالة إدخالات البرنامج في ملف ini.system كما أن بإمكان الخادم إعادة إنشاء نفسه بعد حذفه من الويندوز بإستخدام بعض الملفات المساعدة له في ذلك

خطورة البرنامج :

يمكن عمل تعديلات على الخادم الخاص بالبرنامج من خلال برنامج التحرير الخاص به لذلك فإنه من الواجب البحث في أي مكان ممكن أن يسجل فيه ليعمل تلقائيا يعني أي مكان يمكن وضع أوامر للويندوز ليقوم بتشغيله تلقائيا .

التخلص منه :

١- إفتح الملف ini.win الموجود في مجلد الويندوز وابحث في بداية السطور الأولى من هذاالملف عن أي قيك شبيهة بالقيم التالية :

dll.xxxx =Load أو exe.xxxx=Load أو dll.xxxx = run أو exe.xxxx=run

لاحظ أن xxxx تعني إسم الخادم وإذا عثرت على أي قيمة منها فقم بحذفها

٢- افتح الملف ini.system الموجود في مجلد الويندوز وفي السطر الخامس ستجد السطر التالي :

shell= Explorer.exe ... فإذا كان جهازك مصابا ستجد السطر على هذا الشكل :

shell=Explorer.exe xxxx.exe .... أو shell= Explorer.xxxx exe.dll

مع العلم بأن xxxx هو إسم الخادم الذي من أشهر أسمائه exe.rundll16 و exe.Task_Bar فإذا كان كذلك فقم بمسح إسم الخادم فقط ليصبح السطر : shell= Explorer.exe

٣- إضغط على start ثم تشغيل ثم إكتب regedit لتدخل الى

ملف السجل ثم قم بالدخول تسلسليا على الأتي :

HKEY_LOCAL_MACHINE

Software

Microsoft

Windows

Current Version

داخل المجلد Run إبحث عن إسم الخادم الذي عثرت عليه في مـلف ini.system أو الملف ini.win (في بعض الأحيان قد يتغير إسم الخادم في ملف التسجيل لذلك إبحث عن أي شي غريب) ثم بعد ذلك توجه لمجلد الويندوز وستجد أن حجم الخادم الذي عثرت عليه في ملف التسجيل حوالي ٣٢٨ كيلو بايت إذا كان كذلك عد لنفس المنطقة في ملف التسجيل وقم بحذف القيمة وذلك بالنقر على إسمها وإختيار حذف delete الآن أعد تشغيل الجهاز ثم توجه لمجلد الويندوز وقم بحذف الخادم بالنقر عليه بالزر الأيمن للماوس وإختيار حذف .

تم بحمد الله

أعداد المبرمج:مشتاق طالب رشيد العامري

16-12-2009

بعض طرق الوقاية من الأختراق الألكتروني